Decentralized Contact Directories as a Platform for Blockchain

Consumer friendly Identity & Access Management (IAM) for Networks, Web, Apps, IOT, Smart Contracts, AR/VR and all other domains using crowd sourcing.

DiroToken Sale Economics (internal draft)

January 6, 2018

Diro Foundation

Utility Token - Howy's Test

A Securities Law Framework for Blockchain Tokens

To estimate how likely a particular blockchain token is be a security under US federal securities law

ELEMENT 1: INVESTMENT OF MONEY

Is there an investment of money?				
Characteristic	Points	Explanation	Examples	Y or N
There is no crowdsale. New tokens are given away for free, or are earned through mining	0	Tokens which are not sold for value do not involve an investment of money. For example, if all tokens are distributed for free, or are only produced through mining, then there is no sale for value.	There was never any token sale for Bitcoin. The only way to acquire new bitcoin is via mining. A token which is randomly distributed for free	N
Tokens are sold for value (crowdsale)	100	Tokens which are sold in a crowdsale, at any time, regardless of whether sold for fiat or digital currency (or anything else of value) involve an investment of money	A token which is sold for bitcoin in a crowdsale. A token which is sold for ether in a crowdsale.	Y
			Total for Element 1:	**100**

ELEMENT 2: COMMON ENTERPRISE

What is the timing of the sale?

Characteristic	Points	Explanation	Examples	Y or N
Pre-deployment	70	A sale of tokens before any code has been deployed on a blockchain is more likely to result in a common enterprise where the profits arise from the efforts of others. This is because the buyers are completely dependent on the actions of the developers, and the buyers cannot actually participate in the network until a later time.	A developer has an idea for a new protocol, writes a white paper and does a crowdsale.	N
The protocol is operational on a test network	60	If there is a functioning network there is less likely there is to be a common enterprise where the profits arisef rom the efforts of others. The closer the sale is to launch of the network, the less likley there is to be a common enterprise.	A developer has an idea for a new protocol, writes a white paper and deploys a working test network before doing a crowdsale. .	Y
Live network is operational	50	If the token is sold once there is an operational network using the token, or sold immediately before the network goes live, it is again less likely to result in a common enterprise	The crowdsale is done at the same time the network is launched. .	N

What do token holders have to do in order to get economic benefits from the network?				
Characteristic	Points	Explanation	Examples	Y or N
All token holders will always receive the same returns	25	If returns are paid to all token holders equally (or in proportion to their token holdings) regardless of any action on the part of the token holder, then their interests are more likely aligned in a common enterprise	'HodlToken' holders are automatically paid an amount of ETH each week, based on fees generated by other users of the network 'FoldToken' does not pay any return, and there is no way to earn more tokens within the network (but they can be bought, sold or traded)	N
There is a possibility of varying returns between token holders, based on their participation or use of the network	-20	If token holders' returns depend on their own efforts, and can vary depending on the amount of effort they each put in, then there is less likely to be a common enterprise	'CloudToken' holders can earn more tokens by providing data storage on the network, or can spend tokens to access data storage. Holders who do not provide data storage do not earn any more tokens.	Y
			Total for Element 2:	**40**

ELEMENT 3: EXPECTATION OF PROFIT

What function does the token have?				
Characteristic	Points	Explanation	Examples	Y or N
Ownership or equity interest in a legal entity, including a general partnership	100	Tokens which give, or purport to give, traditional equity, debt or other investor rights are almost certainly securities. *If one or more of these characteristics apply, the token is almost certainly a security, notwithstanding the results of the other elements*	A developer releases and sells 100 'BakerShares' tokens. Each token entitles the holder to 1 share in Baker, Inc. A developer releases and sells 100 'BakerProfit' tokens. Each token entitles the holder to 1% of the profits of Baker, Inc. for the next year. A developer releases and sells 100 'BakerDebt' tokens. Each token entitles the holder to principal and interest repayments based on the initial token sale price.	N
Entitlement to a share of profits and/or losses, or assets and/or liabilities	100			N
Gives holder status as a creditor or lender	100			N
A claim in bankruptcy as equity interest holder or creditor	100			N
A right to repayment of purchase price and/or payment of interest	100			N
No function other than mere existence	100	A token which does not have any real function, or is used in a network with no real function, is very likely to be bought with an expectation of profit from the efforts of others, because no real use or participation by token holders is possible. Voting rights alone do not constitute real functionality.	A developer releases and sells 100,000 'SocialCoin' tokens to fund the development of a new Social Network. However, SocialCoin is not required to access the network and has no real function after the sale.	N
Specific functionality that is only available to token holders	0	A token which has a specific function that is only available to token holders is more likely to be purchased in order to access that function and less likely to be purchased with an expectation of profit.	'CloudToken' is the only way to access and use a decentralized file storage network.	Y

Does the holder rely on manual, off-blockchain action to realize the benefit of the token?				
Characteristic	Points	Explanation	Examples	Y or N
Manual action is required outside of the network (e.g. off-blockchain) in order for the holder to get the benefit of the token	80	A token whose value depends on someone taking specific manual action outside of the network means that the token is not functional in and of itself. Instead, the token relies on a level of trust in a third party taking action off-blockchain. This sort of token is more likely to be bought for speculation - i.e. the expectation of profits.	A developer releases and sells 'FreightCoin', which will allow the holder to pay FreightCoin to access capacity on a new real-world freight network. The network relies on legal contractual relationships and manual actions. (This alone does not make FreightCoin a security)	N
All functionality is inherent in the token and occurs programmatically	0	A token which is built with all the necessary technical permissions means that the token holder does not rely on manual actions of any third party. This means that the buyers are more likely to purchase the token for use rather than with the expectation of profit from the efforts of others.	Holders of 'SongVoteToken' can sign transactions on the network as votes for their favorite new songs and earn rewards for doing so.	Y

What is the timing of the sale?				
Characteristic	Points	Explanation	Examples	Y or N
Pre-deployment	20	A sale of tokens before any code has been deployed on a blockchain is more likely to result in buyers purchasing for speculative reasons with the expectation of profit, rather than practical use cases.	A developer has an idea for a new protocol, writes a white paper and does a crowdsale.	N
The protocol is operational on a test network	10	If the sale occurs after code has been deployed and tested, the token is closer to being able to be used	A developer has an idea for a new protocol, writes a white paper and develops a working test network before doing a crowdsale.	Y
Live network is operational	0	If the token is sold once there is an operational network using the token, or immediately before the network goes live, it is more likely to be purchased with the intention of use rather than profit.	The live network is launched before the crowdsale.	N

Can the token holders exercise real and significant control via voting?				
Characteristic	Points	Explanation	Examples	Y or N
Token holders as a whole are able to control the development team's access to funds	-20	If the collective approval of token holders is required in order for the development team to access the funds raised in the crowdsale, then any value realized by the token holders is more closely tied to their own decisions, and less reliant on the efforts of others.	A development team sells 100,000 Tokens for a total of 100,000 ETH. 50,000 ETH will be released from the token contract to the development team immediately, but the remainder is only released once milestones are met, which requires approval of a majority of the token holders each time. If the milestones are never met, the remaining ETH will be returned to the token holders.	N
Token holders as a whole are able to vote on significant decisions for the protocol	-10	If the collective approval of token holders is required in order to make significant changes to the protocol, then any value realized by the token holders is more closely tied to their own decisions, and less reliant on the efforts of others.	Changes to the protocol require a vote by token holders.	Y

Note: Voting rights must be in addition to functionality. A token with voting rights alone and no other real functionality is very likely to satisfy element 3

How is the token sale marketed?				
Characteristic	Points	Explanation	Examples	Y or N
Marketed as an 'Initial Coin Offering' or similar	50	It is not possible to prevent some buyers from buying a token purely for speculation. However, marketing the token as an investment leads buyers to believe they can profit from holding or trading the token, rather than from using the token in the network. Using terms like 'Initial Coin Offering' or 'ICO', and investment-related language like 'returns' and 'profits' encourages buyers to buy a token for speculation, rather than use.	'ProfitCoin' includes potential of 'high ROI' and 'investor profits' in its marketing material.	N
Marketed as a Token Sale	0	Marketed as a sale of tokens which give the right to access and use the network		Y
There is no economic return possible from using the network	-100	If there is genuinely no economic return possible for the token holders, then there is unlikely to be a common enterprise. This will be rare.	Backers contribute to a cause and receive a 'thank you' token which has no economic value.	N

Results			
Guide		Your Results	
Total Points	How likely is the element to be satisfied?		
0 or less	Very unlikely	Total for Element 1	100
1 - 33	Unlikely	Total for Element 2	40
34 - 66	Equally likely and unlikely	Total for Element 3	0
67 - 99	Likely	Overall Risk Score	0
100 or more	Very likely		

A token will only be a security if it satisfies all three elements. The higher the point score for each element, the more likely the element is to be satisfied. For many blockchain tokens, the first two elements of the Howe'y test are likely to be met. The third element has the most variables and the most different outcomes depending on the characteristics of the particular token.

Important notes

Please remember that this methodology produces nothing more than an estimate. The Overall Risk Score and the categories of likelihood are a guide only.

The Howe'y test has not yet been directly applied by the courts to any digital currency or blockchain token. The Howe'y test as applied by the courts does not involve any points-based calculation. The points system is intended as a guide - to highlight the characteristics of a token which are relevant to the securities law analysis.

This Framework should be read together with the full legal analysis. This Framework and the full legal analysis may be updated in the future as the law in this area develops.

You should not rely on this Framework as legal advice. It is designed for general informational purposes only, as a guide to certain of the conceptual considerations associated with the narrow issues it addresses. You should seek advice from your own counsel, who is familiar with the particular facts and circumstances of what you intend and can give you tailored advice. This Framework is provided "as is" with no representations, warranties or obligations to update, although we reserve the right to modify or change this Framework from time to time. No attorney-client relationship or privilege is created, nor is this intended to be attorney advertising in any jurisdiction.

1. Proposed Structure

We will register a limited company in Singapore (ACRA registered) to run the non-profit foundation that will operate the functioning of DiroToken. All Token issuances will be compliant under Singapore Law and subject to arbitration under the jurisdiction of Singapore. All KYC & AML guidelines to be followed that will include:

- Verification of investors.
- Investors to be checked against multiple government & financial industry AML watch lists.

2. Know Your Customer (KYC) Guidelines

We will register a limited company in Singapore (ACRA registered) to run the non-profit foundation that will operate the functioning of DiroToken. All Token issuances will be compliant under Singapore Law and subject to arbitration under the jurisdiction of Singapore. All KYC & AML guidelines to be followed that will include:

- Verification of investors
- Investors to be checked against multiple government & financial industry AML watch lists

To invest in the token sale the following KYC steps will be taken.

FOR US RESIDENTS

- Must not be a New York state resident
- A U.S. social security number
- Evidence of your net worth or income such as W2s, financial statements, asset appraisals, or a letter from your lawyer, accountant, investment advisor or investment broker. Documents must be dated in the last 30 days
- A U.S. bank account (you'll be required to pre-fund today) OR a BTC or ETH wallet with funds to cover your desired investment amount

FOR NON-U.S. RESIDENTS

- A legible scan of the first page of your passport or other government-issued photo ID
- Evidence of your net worth or income such as financial statements, asset appraisals, or a letter from your lawyer, accountant, investment advisor or investment broker.
- A U.S. bank account (you'll be required to pre-fund today) OR a BTC or ETH wallet with funds to cover your desired investment amount

3. Anti Money Laundering (AML) Guidelines

We will run the list of investors against the list of Specially Designated Nationals and Blocked Persons List of the Office of Foreign Assets Control of the United States Department of the Treasury ("OFAC"). There are agencies that provide APIs to check information against OFAC & other Financial Industry watch lists.

4. Compliance Status

Aspect	Component	Level I	Level II	Level III
Cryptographic Asset Management				
Key / Seed Generation	Operator-created Key / Seed			✔
	Creation methodology is validated			✔
	DRBG Compliance			
	Entropy Pool			
Wallet Creation	Unique address per transaction	✔		
	Multiple keys for signing			✔
	Redundant key for recovery			✔
	Deterministic wallets			
	Geographic distribution of keys			✔
	Organizational distribution of keys			✔
Key Storage	Primary keys are stored encrypted			✔
	Backup key exists			✔
	Backup key has environmental protection			✔
	Backup key is access-controlled			
	Backup key has tamper-evident seal			✔
	Backup key is encrypted			✔
Key Usage	Key access requires user/pass/nth factor			
	Keys are only used in a trusted environment			✔
	Operator reference checks			✔
	Operator ID checks			✔
	Operator background checks			✔
	Spends are verified before signing			✔
	No two keys are used on one device			✔
	DRBG Compliance			

Aspect	Component	Level I	Level II	Level III
Key Compromise Protocol (KCP)	KCP Exists	✔		
	KCP Training + Rehearsals			
	Keyholder Grant/Revoke Policies & Procedures			
	Requests made via Authenticated Communication Channel			✔
	Grant/Revoke Audit Trail			
Operations				
Security Audits / Pentests	Security Audit	✔		
Data Sanitization Policy (DSP)	DSP Exists	✔		
	Audit Trail of all media sanitization			
Proof of Reserve (PoR)	Proof of Reserve Audits			✔
Audit Logs	Application Audit Logs	✔		
	Backup of Audit Logs			✔

5. Community messaging & Wallet Address Security

Slack

Due to ever-increasing amounts of potential threats, we will not be using Slack channels. You will be able to track all of our updates on #Announcements channel, where we will post frequently asked questions and any updates regarding the crowdsale.

Once the messaging will be disabled, you will have an option to PM us with your questions (Only PM user “DIRO” on Slack). Please note, that we will try to respond as soon as possible, but it may take us a few hours to do that.

TIP: Never trust any messages from Slackbot, as anyone can send messages with it. Diro was never hacked, and we will never ask you to enter any information about unlocking your wallet.

Telegram

Once our Slack will be disabled, you will have an option to join our Telegram group, and ask any questions there.

If you will receive a PM from anyone pretending to be DIRO, we recommend you to check the validity of the person in the DIRO group, or you can DM us on Twitter.

Email newsletter

We will never send you our wallet address in the email, so don't trust anyone that will do otherwise—you will only be able to see our address in www.diro.io (top left corner, click "Join Crowdsale")

Facebook

Throughout the crowdsale, we will have a live Facebook video, that we recommend you to watch. In case of any hacking attempts or any troubles, you will be the first one to know, if you will watch the livestream. During the livestream, we will also provide you with any updates (if we reach the soft-cap or the hard cap and more).

Diro.eth

We will also be updating the wallet address on the block chain to avoid mistyping of the address.

Website

Remember that the only legitimate website is https://www.diro.io/ . If you will receive any other links, please make sure that you are entering the correct website, by simply checking the link at the top of your browser and is SSL certified.

Double Check the Address

A few days before the beginning of the ICO, we will release the DIRO that will the exact address of our wallet. Please check the app and make sure that the digits you will see on Diro.io website will match.

Website Security

The website is SSL certified to support HHTPS connection as standard. All admin logins have been setup with 2 factor authentication and ACLs.

Scans Continuously
Unlike other providers that scan your site merely once every day, SiteLock INFINITY scans the site continually all day. Once the site scan completes, it scans again — as often as multiple times every hour ensuring maximum coverage and protection. SiteLock is the only cloud-based security provider today that can deliver this level of scanning protection.

Finds Malware and Removes It Immediately
Due to INFINITY high scanning frequency, malware is found and removed essentially the moment it hits, thereby mitigating its spread to other areas of the network.

Detects and Remediates Vulnerabilities
INFINITY scans your website — any and all malware is detected from the inside-out, as well as the outside-in. Scans look for sophisticated vulnerabilities — like Cross Site Scripting (XSS) and SQL Injections (SQLi). All sophisticated back-door vulnerability patches are included too.

Diro Foundation

www.diro.io
ico@diro.io